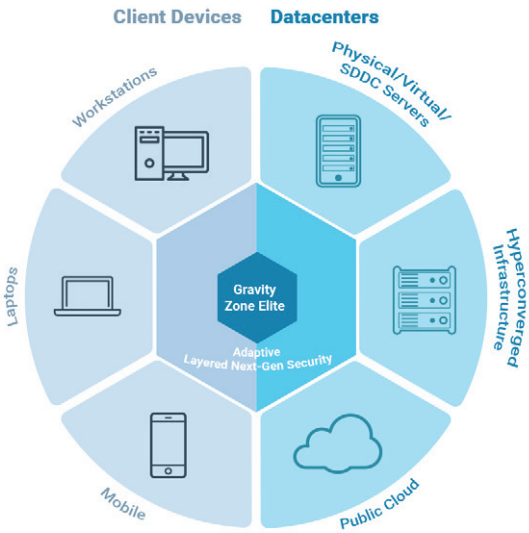
Bitdefender GravityZone Elite Suite

Die mehrschichtige Sicherheitsplattform der nächsten Generation

Die Bitdefender GravityZone Elite Suite schützt Unternehmen vor der ganzen Bandbreite hochkomplexer Cybergefahren – schnell und präszise. Elite vereint Bitdefenders bewährte mehrschichtige Sicherheitsstrategie mit Tools und Technologien der nächsten Generation. So liefert die Suite höchste Leistung bei größtmöglichem Schutz für Endpunkte aller Art im gesamten Firmennetzwerk: Arbeitsplatzrechner, Laptops, Smartphones, physische und virtuelle Server.

GravityZone Elite sorgt für durchgehende Sicherheit der gesamten IT-Umgebung, damit kein Endpunkt ungeschützt bleibt und so als Einfallstor für Schad-Software dienen könnte. Das Ganze basiert auf einer einfachen, integrierten Architektur mit zentraler, einheitlicher Verwaltung für Endpunkte und Rechenzentren gleichermaßen. Die Verwaltungskonsole gibt es in einer Cloud-Version und in einer lokalen Version. So ist für jede IT-Umgebung das Richtige dabei.



HIGHLIGHTS

- Dateilose Malware-Angriffe erkennen und blockieren
- Skript-basierte Angriffe abwehren
- Unbekannte Malware noch vor der Ausführung entpacken und analysieren
- Ein Agent für alles, schlank und ressourcenschonend
- Integrierte Verwaltungskonsole für physische und virtuelle Endpunkte

Endpunktschutz

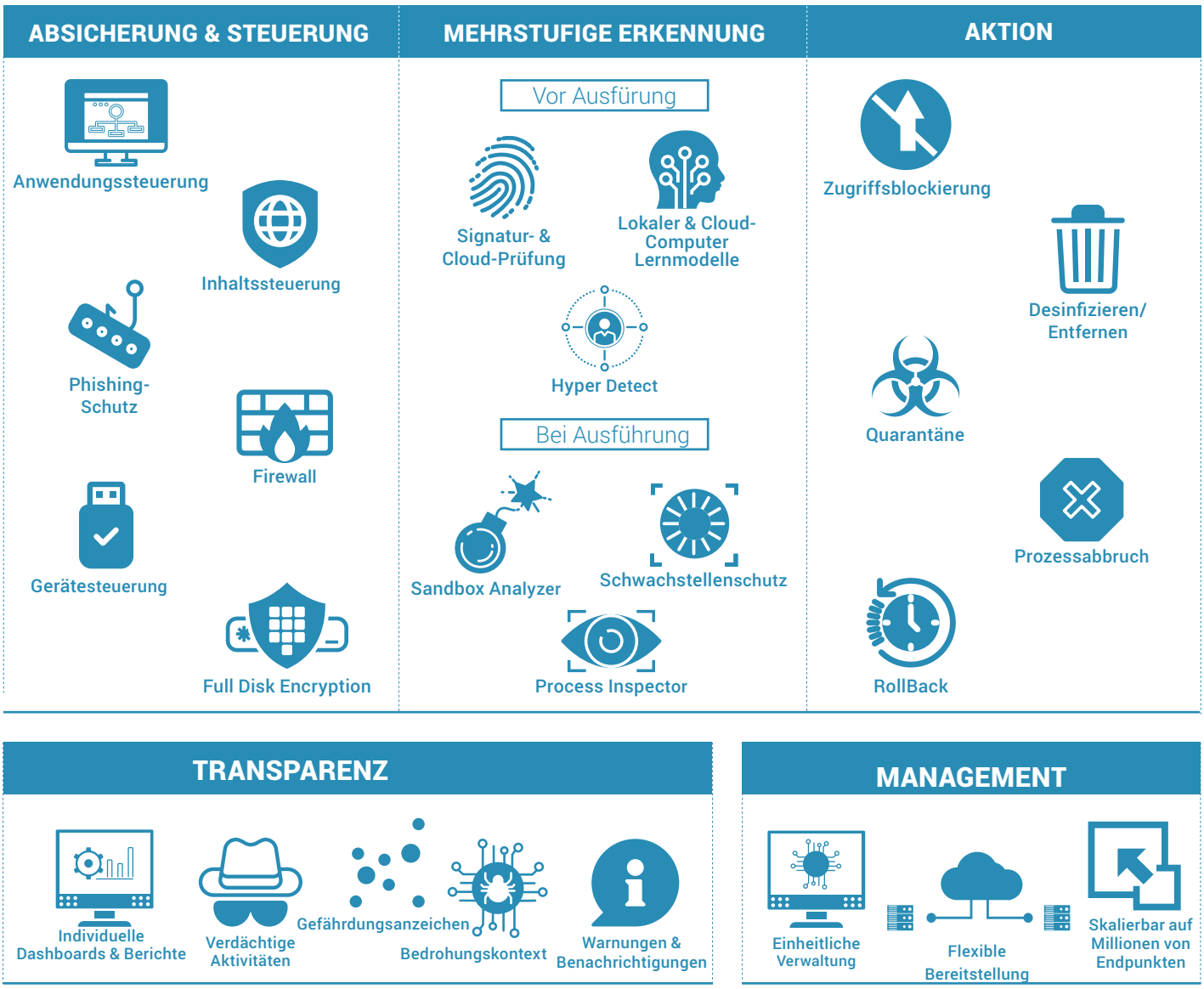
Bitdefender Endpoint Security HD – die Endpunktsicherheitskomponente von GravityZone Elite – schützt Unternehmen vor der gesamten Bandbreite hochkomplexer Cybergefahren – schnell, unkompliziert, präzise und ressourcenschonend. Diese hochmoderne Lösung macht es unnötig, mehrere Endpunktsicherheitslösungen auf derselben Maschine laufen zu lassen, da sie vorbeugende Maßnahmen mit mehrstufigen signaturunabhängigen Erkennungstechniken und automatischer Reaktionsmöglichkeit vereint.

Hauptvorteile

Erkennung und Schutz vor dem gesamten Spektrum bekannter und unbekannter Schad-Software
Endpoint Security HD verhindert selbst raffinierte Bedrohungen und unbekannte Malware, wie z. B. Ransomware, die traditionelle Lösungen nicht erkennen. Hochaggressive Angriffe wie PowerShell, Skript-basierte oder dateilose Angriffe und andere hochkomplexe Malware können zuverlässig gefunden und noch vor ihrer Ausführung blockiert werden.

Dateilose Malware finden und blockieren
Dateilose Malware-Angriffe führen Schad-Codes direkt im Arbeitsspeicher aus. Da keine Datei auf der Festplatte gespeichert wird, können die meisten Virenschutzlösungen sie nicht finden – denn diese konzentrieren sich oft ausschließlich auf die Dateianalyse. Bitdefender setzt den leistungsstarken Schwachstellenschutz, HyperDetect™ und Process Inspector ein, um dateilose Angriffe zu finden, zu blockieren und unschädlich zu machen.

Makro- und Skript-basierte Angriffe stoppen
Hierbei nutzen Angreifer MS-Office-Makros aus, um über Windows-Verwaltungstools wie PowerShell Skripte auszuführen und Schad-Codes herunterzuladen. Da es sich hierbei um „vertrauenswürdige" Windows-Tools handelt, untersuchen die meisten Endpunktsicherheitsprodukte, selbst sogenannte Next-Gen-Virenschutzprodukte, Skripte in PowerShell, WMI, Javascript oder anderen Interpretern nicht genau. Bitdefender prüft und sichert Skripte durch eine Befehlszeilenanalyse, alarmiert Administratoren und blockiert die Ausführung verdächtiger Skripte.



Automatisierte Reaktion und Bereinigung von Bedrohungen
Sobald eine Bedrohung gefunden wurde, wird sie sofort von Endpoint Security HD neutralisiert, u. a. durch Abbruch von Prozessen, Verschieben in die Quarantäne, Entfernen und Rückgängigmachen von schädlichen Änderungen. Die Lösung tauscht in Echtzeit Daten mit dem GPN (Global Protective Network) aus, Bitdefenders Cloud-basiertem Gefahrenanalysedienst. So können ähnliche Angriffe überall auf der Welt verhindert werden.

Mehr Transparenz und Kontext zu bestimmten Gefahren
Bitdefender Endpoint Security HD zeichnet sich dadurch aus, dass es verdächtige Aktivitäten aufspürt und frühzeitig an die Administratoren meldet; solche Aktivitäten sind zum Beispiel ungewöhnliche Anfragen des Betriebssystems, ausweichende Aktionen und Verbindungen zu Command-and-Control-Servern.

Mehr Effizienz im Betrieb durch nur einen einzigen Agenten und eine integrierte Konsole
Da Bitdefender nur einen einzigen integrierten Endpunktsicherheitsagenten einsetzt, kommt es nicht zur Agentenüberfrachtung. Der modulare Aufbau bietet höchste Flexibilität und lässt Administratoren Sicherheitsrichtlinien einrichten. GravityZone passt das Installationspaket automatisch und individuell an und minimiert so den Ressourcenverbrauch des Agenten. GravityZone ist von Grund auf als einheitliche, umfassende Sicherheitsverwaltungsplattform ausgelegt die physische, virtuelle und Cloud-Umgebungen gleichermaßen zuverlässig schützt.

Bestandteile

Machine Learning
Verfahren für das maschinelle Lernen nutzen gut konfigurierte Maschinenmodelle und Lernalgorithmen, um komplexe Angriffe vorherzusagen und aufzuhalten. Die Bitdefender-Modelle für Machine Learning verwenden rund 40.000 statische und dynamische Eigenschaften und werden fortlaufend anhand von vielen Milliarden unbedenklichen und schädlichen Dateien weiter entwickelt, die von mehr als 500 Millionen Endpunkten weltweit bezogen wurden. So kann die Effektivität der Malware-Erkennung erheblich gesteigert und die Zahl der Fehlalarme minimiert werden.

HyperDetect
Diese neue Sicherheitsschicht verfügt über lokale Machine Learning Modelle und hochentwickelte Heuristiken, die mit enormer Präzision Hacker-Tools, Exploits und Malware-Obfuskationstechniken erkennen und diese raffinierten Bedrohungen blockieren, noch bevor sie ausgeführt werden. Die Software spürt auch Einbringungstechniken und Websites auf, die Exploit-Kits hosten, und blockiert verdächtigen Internetdatenverkehr. Mit HyperDetect können Netzwerkadministratoren die Sicherheitsstrategie gezielt gegen die für Ihr Unternehmen relevantesten Cyber-Gefahren

konfigurieren. Mit der Option „Report Only“ können Administratoren ihre neue Sicherheitsrichtlinie gestaffelt testen und überwachen, bevor sie sie diese flächendeckend implementieren. So können lästige Betriebsunterbrechungen vermieden werden. HyperDetect bietet eine Kombination aus hoher Transparenz und wirkungsvollem Blockierverhalten, die es so nur bei Bitdefender gibt: Die Software kann so eingerichtet werden, dass auf normaler und toleranter Sicherheitsstufe blockiert wird, während auf aggressiver Sicherheitsstufe weiterhin Warnmeldungen ausgegeben werden. So werden schon erste Anzeichen von Cyber-Gefahren frühzeitig erkannt.

Im Endpunkt integrierter Sandbox-Analyzer
Diese leistungsstarke Sicherheitsschicht analysiert verdächtige Dateien im Detail, untersucht Malware in einer isolierten virtuellen Umgebung, die von Bitdefender gehostet wird, analysiert dort ihr Verhalten und gibt bei schädlichen Vorgängen einen Bericht aus. Der im GravityZone-Endpunkt-Agenten integrierte Sandbox-Analyzer übermittelt verdächtige Dateien automatisch zur Analyse. Nach einer Schädlich-Einstufung des Sandbox Analyzer blockiert Endpoint Security HD die schädliche Datei automatisch unternehmensweit auf allen Systemen. Über die automatische Übermittlungsfunktion können Sicherheitsbeauftragte zwischen Überwachungsmodus und Blockiermodus wählen (und wechseln). Im letzteren wird der Zugriff auf Dateien verweigert, bis eine Einstufung als unbedenklich erfolgt ist. Administratoren können Dateien auch manuell zur Analyse übermitteln. Die detaillierten und umfassenden Informationen des Sandbox-Analyzers bieten nützlichen Kontext zu einzelnen Bedrohungen und helfen so, das Verhalten verschiedener Bedrohungen besser zu verstehen.

Leistungsstarker Schwachstellenschutz
Die Exploit-Abwehr-Technologie schützt den Speicher und besonders anfällige Anwendungen wie Browser, Dokumentanzeigeprogramme, Mediendateien und Laufzeit (z. B. Flash, Java). Komplexe Mechanismen überwachen Routinen für den Speicherzugriff, um Exploit-Verfahren wie API-Caller-Verification, Stack Pivot, Return-Oriented Programming (ROP) und Viele mehr zu erkennen und abzuwehren.

Process Inspector
Der Process Inspector vertraut nichts und niemandem und überwacht durchgehend jeden einzelnen Prozess, der im Betriebssystem läuft. Die Software spürt verdächtige Aktivitäten oder ungewöhnliches Prozessverhalten auf, z. B. Verbergen des Prozesstyps, Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, Ablegen von Dateien, Verbergen vor Anwendungen zur Prozessübersicht und mehr. Der Process Inspectorwendet angemessene Bereinigungsaktionen an, z. B. die Beendigung des Prozesses oder die Rückgängigmachung von Änderungen, die dieser Prozess vorgenommen hat. Er hat sich dabei als äußerst effektiv bei der Erkennung unbekannter, komplexer Malware sowie dateiloser Angriffe und Ransomware erwiesen.

Phishing-Schutz und Web-Sicherheits-Filter
Mithilfe von Web-Sicherheitsfiltern kann der eingehende Internet-Datenverkehr (einschließlich SSL-, HTTP- und HTTPS-Datenverkehr) gescannt werden, um zu verhindern, dass Malware auf Endpunkte heruntergeladen wird. Der Phishing-Schutz blockiert automatisch alle Phishing-Seiten und auch andere betrügerische Webseiten.

Full Disk Encryption
Vollständige Laufwerksverschlüsselung, verwaltet durch GravityZone, auf der Basis von Windows BitLocker und Mac FileVault. GravityZone nutzt die Vorteile der in die Betriebssysteme eingebauten Technologien. FDE ist als Add-on verfügbar, separat lizenziert.

Steuerung und Absicherung von Endpunkten
Die richtlinienbasierte Endpunktsteuerung umfasst die Firewall, die Gerätesteuerung mit USB-Scans sowie die Inhaltssteuerung mit URL-Kategorisierung.

Reaktion und Isolierung
GravityZone bietet die besten Bereinigungsfunktionen auf dem Markt. Die Software blockiert/isoliert Bedrohungen automatisch, terminiert bösartige Prozesse und macht Änderungen rückgängig.

Sicherheit für Rechenzentren

GravityZone Security for Virtualized Environments (SVE) macht sich die mehrschichtige Sicherheitsarchitektur von Bitdefender Endpoint Security HD zunutze, um Unternehmen branchenführende Sicherheit für Server, VDI und die Cloud zu bieten – und das bei gleichzeitiger Steigerung der Infrastrukturleistung und Betriebseffizienz. GravityZone SVE ist eine Enterprise-Lösung, die für die Anforderungen großer Rechenzentren entwickelt wurde.

Hauptvorteile

Flexibilität
Mit SVE lässt sich die Sicherheit eines Rechenzentrums sowohl bei der Einrichtung als auch beim täglichen Betrieb über den gesamten Lebenszyklus automatisieren, selbst in hochgradig dynamischen Umgebungen. Es lässt sich mit VMware (vCenter, vShield, NSX), Citrix XenCenter und Nutanix Enterprise Cloud Platform integrieren und lässt sich schnell und automatisiert installieren und einrichten.

Effizienter Betrieb
Das GravityZone Control Center ist die zentrale Schaltstelle, die alles von der Installation über die Verwaltung bis hin zu Upgrades extrem unkompliziert macht und volle Transparenz aller virtuellen und physischen Server und Arbeitsplatzrechner gewährt. Dank der zentralisierten Erstellung und automatischen Anwendung von Sicherheitsrichtlinien wird der IT-Betrieb optimiert und gleichzeitig die Compliance verbessert.

Verbesserte Infrastrukturnutzung
Dank zentralisierter Scans und einem schlanken Agenten werden Festplatten-, Arbeitsspeicher, CPU- und E/A-Anforderungen an Host-Server drastisch gesenkt, was eine höhere VM-Dichte und einen besseren ROI der IT-Infrastruktur beteutet.

Universelle Kompatibilität
Durch die Kompatibilität mit sämtlichen Virtualisierungsplattformen (z. B. VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM oder Nutanix® Acropolis), Microsoft Active Directory sowie Windows®- und Linux®-Gastbetriebssystemen macht GravityZone die Installation, Endpunkterkennung und Richtlinienverwaltung zum Kinderspiel.

Unbegrenzte lineare Skalierbarkeit
Durch den Einsatz mehrerer SVAs kann die Scan-Kapazität erhöht werden, wenn das durch ein Anwachsen des Rechenzentrums oder der Zahl der VMs nötig werden sollte. Wenn eine SVA der Last nicht mehr gerecht wird, können ganz einfach neue hinzugefügt werden.

Mehrschichtige Sicherheit der nächsten Generation
GravityZone Security for Virtualized Environments umfasst alle essentiellen Sicherheitsschichten von Endpoint Security wie HyperDetect, Sandbox Analyzer und Methoden zur Erkennung dateiloser Angriffe. So bleiben alle im gesamten Rechenzentrum gespeicherten oder verarbeiteten digitalen Unternehmenswerte sicher.

Security for iOS and Android Mobile Devices

Die Lösung ist darauf ausgelegt, das BYOD-Konzept (Bring Your Own Device) kontrolliert zu begleiten, indem sie die einheitliche Durchsetzung von Sicherheitsrichtlinien auf allen Geräten im Netzwerk sicherstellt. So werden die Mobilgeräte zuverlässig kontrolliert und die darauf gespeicherten sensiblen Unternehmensdaten geschützt. Der administrative Aufwand wird reduziert, da jederzeit Klarheit darüber herrscht, welche Geräte den Richtlinien entsprechen und welche nicht.

Security for Exchange Servers

Die Lösung bietet mehrere Sicherheitsschichten für den E-Mail-Verkehr: Spam-Schutz, Phishing-Schutz, Virenschutz und Malware-Schutz mit Verhaltensanalyse, Zero-Day-Schutz und E-Mail-Verkehr-Filterung (inkl. Anhangs- und Inhaltsfilterung). Malware-Scans können von den geschützten Mail-Servern auf zentrale Sicherheitsserver ausgelagert werden. Durch die zentrale Verwaltung und Berichterstattung können einheitliche Richtlinien für Endpunkte und den Nachrichtenverkehr festgelegt werden.

GravityZone Control Center

GravityZone Control Center ist eine integrierte, zentrale Verwaltungskonsole für sämtliche Sicherheitskomponenten mit denen Endpunkte, Rechenzentren, Exchange-Server und Mobilgeräte geschützt werden. Sie kann in der Cloud gehostet oder lokal installiert werden. In dieser GravityZone-Verwaltungszentrale sind mehrere Rollen zusammengefasst: Datenbank-Server, Kommunikationsserver, Update-Server und Web-Konsole. In größeren Unternehmen kann sie so konfiguriert werden, dass sie mehrere virtuelle Appliances mit mehreren Instanzen bestimmter Rollen und einen integrierten Lastenausgleich verwendet, um Skalierbarkeit und Hochverfügbarkeit sicherzustellen.

Detaillierte Systemanforderungen finden Sie unter https://www.bitdefender.de/business/elite-security.html

BD-NGZ-Oct.20.2017-1f-ar
Bitdefender-NGZ-Elite-Datasheet-creat2088-A4-de_DE